Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/006014

International filing date: 24 February 2005 (24.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/549,357
Filing date: 02 March 2004 (02.03.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1301300

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 25, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/549,357*
FILING DATE: *March 02, 2004*
RELATED PCT APPLICATION NUMBER: *PCT/US05/06014*

Certified by

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16 (01-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV406600030

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Anton	Zavriyev	Swampscott, MA

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ Customer Number: 36522

OR

☐ Firm or Individual Name					
Address					
Address					
City		State		Zip	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 10
☒ Drawing(s) *Number of Sheets* 2
☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number _____
☐ Other (specify) _____

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fees.
☒ The Director is herby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 502992
☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($): $80-

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE Joseph E Gortych
TYPED or PRINTED NAME Joseph E. Gortych
TELEPHONE 802-655-7222

Date March 2, 2004
REGISTRATION NO. 41,791 *(if appropriate)*
Docket Number: 022B-03P

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

3

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 80—

Complete if Known	
Application Number	N/A
Filing Date	March 2, 2004
First Named Inventor	ZAVRIYEV, Anton
Examiner Name	—
Art Unit	—
Attorney Docket No.	022B-03P

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 502992

Deposit Account Name: MagiQ Technologies, Inc.

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	80

SUBTOTAL (1) ($) 80—

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X =
Independent Claims		- 3** =		X =
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) N/A

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) Ø

SUBMITTED BY

(Complete *(if applicable)*)

Name (Print/Type)	Joseph E. Gortych	*Registration No. (Attorney/Agent)*	41,791	*Telephone*	8026557222
Signature	Joseph E. Gortych			*Date*	March 2, 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MODULATOR AUTOCALIBRATION METHODS FOR QKD

Field of the Invention

The present invention relates to quantum cryptography, and in particular relates to methods for automatically calibrating modulators in a two-way quantum key exchange (QKD) system.

Background of the Invention

Quantum key distribution involves establishing a key between a sender ("Alice") and a receiver ("Bob") by using weak (e.g., 0.1 photon on average) optical signals transmitted over a "quantum channel." The security of the key distribution is based on the quantum mechanical principal that any measurement of a quantum system in unknown state will modify its state. As a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the quantum signal will introduce errors into the transmitted signals, thereby revealing her presence.

The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). Specific QKD systems are described in publications by C.H. Bennett et al entitled "Experimental Quantum Cryptography" and by C.H. Bennett entitled "Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. Lett. 68 2121 (1992).

The general process for performing QKD is described in the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 2001, in Section 2.3, pages 27-33. During the QKD process, Alice uses a random number generator (RNG) to generate a random bit for the basis ("basis bit") and a random bit for the key ("key bit") to create a qubit (e.g., using polarization or phase encoding) and sends this qubit to Bob.

The above mentioned publications by Bennet each describe a so-called "one-way" QKD system wherein Alice randomly encodes the polarization or phase of single photons at one end of the system, and Bob randomly measures the polarization or phase of the photons at the other end of the system. The one-way system described in the Bennett 1992 paper is based on two optical fiber Mach-Zehnder interferometers. Respective parts of the interferometric system are accessible by Alice and Bob so that each can control the phase of the interferometer. The interferometers need to be actively stabilized to within a portion of quantum signal wavelength during transmission to compensate for thermal drifts.

U.S. Patent No. 6,438,234 to Gisin (the '234 patent), which patent is incorporated herein by reference, discloses a so-called "two-way" QKD system that is autocompensated for polarization and thermal variations. Thus, the two-way QKD system of the '234 patent is less susceptible to environmental effects than a one-way system.

However, even in autocompensated QKD systems, only the optics layer is autocompensated. As it turns out, drifts can and do occur in the electronics necessary to stably operate the QKD system. For example, in a phase-encoding QKD system, if the voltage used to set the phase modulators drifts over time, then the phase imparted to the optical pulses will drift over time. The same is true for polarization modulators in polarization-encoding systems. This drift results in the pulses not having precise phase or polarization modulation, which reduces the ability to detect the encoded pulses.

Also, when performing the analysis of the basis measurements under the particular (e.g., the BB84 protocol), there needs to be a 50-50 chance of Bob's detectors detecting signals measured in a basis different from Alice's basis. To the extent this probability differs from 50-50, an eavesdropper has a potential advantage because the uncertainty associated with a "wrong" basis measurement is reduced.

Summary of the Invention

The present invention sets forth methods for autocompensating the modulators in a two-way QKD system. One aspect of the invention includes setting Bob's modulator voltage V_B to a positive value and then adjusting Alice's modulator voltage V_A in both the positive and negative direction to obtain overall phase modulations that show up in one or the other of two detectors. Bob's modulator voltage is then set to a negative value ($-V_B$) and the process repeated. When all of the basis voltages are set, the QKD system is operated with purposely selected incorrect bases at Bob and Alice to verify the appropriate probability of photon arrival at the detectors. If required, the modulator voltages are adjusted and the technique repeated until an appropriate detector count distribution is obtained for the incorrect measurement bases.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of a two-way QKD system;

FIG. 2 is a flow diagram of an example embodiment of the method of performing modulator autocalibration as described in connection with the two-way QKD system of FIG. 1.

Detailed Description of the Invention

The present invention relates to quantum cryptography, and in particular relates to systems and methods for performing phase or polarization modulation in quantum key exchange (QKD) system. The ideal operation of a two-way QKD system is described immediately below, followed by descriptions of example embodiments of the timing set-up and modulator autocalibration methods that enable ideal or close-to-ideal operation of a QKD system on an ongoing basis.

Two-way QKD system

FIG. 1 is a schematic diagram of a two-way QKD system 100. Bob includes laser 12 that emits light pulses P0. Laser 12 is coupled to a time-multiplexing/demultiplexing (M/D) optical system 104. M/D optical system 104

receives input pulses P0 from laser 12 and splits each pulse into two time-multiplexed pulses P1 and P2. Likewise, optical system 104 receives from Alice (discussed below) pairs of time-multiplexed pulses and combines (interferes) them into a single pulse. Bob also includes a phase modulator MB coupled to an M/D optical system on the side opposite laser 12. Optical fiber link FL is coupled to phase modulator MB and connects Bob to Alice. Bob also includes a voltage controller 44 coupled to modulator MB, and a random number generator (RNG) unit 46 coupled to the voltage controller.

Bob also includes two detectors 32a and 32b coupled to M/D optical system 104, and a controller 50 operatively (e.g., electrically) coupled to laser 12, detectors 32a and 32b, voltage controller 44 and to RNG unit 46.

Alice includes a phase modulator MA coupled at one end to optical fiber link FL and at the opposite end to a Faraday mirror FM. Alice also includes voltage controller 14 coupled to modulator MA, and random number generator (RNG) unit 6 coupled to the voltage controller. Alice further includes controller 20 coupled to RNG unit 16 and to voltage controller 14.

Bob's controller 50 is coupled (optically or electronically) to Alice's controller 20 via synchronization channel SL to synchronize the operation of Alice and Bob. In particular, the operation of the phase modulators MA and MB is coordinated by controllers 20 and 50 exchanging synchronization signals SS. In an example embodiment, the operation of the entire system is controlled from either controller 20 or controller 50.

In the operation of QKD system 100, Bob's controller 20 sends a signal S0 to laser 12, which in response thereto initiates a relatively strong, short laser pulse P0, which is then attenuated by an optional variable optical attenuator VOA 13B. The (weak) pulse P0 arrives at M/D optical system 104, which splits the pulse into two weak pulses, P1 and P2, having orthogonal polarization. Pulse P1 goes directly towards Alice while P2 is delayed. Pulses P1 and P2 pass through MB (which remains inactivated at this point), and the pulses travel down the fiber to Alice.

Note that in another embodiment of system 100, pulses P0 and P1 can be relatively strong pulses that are attenuated by Alice using a VOA 13A located at Alice, wherein the pulses are attenuated to make them weak (quantum) pulses prior to them returning to Bob.

The pulses pass through Alice's modulator MA and reflect off of Faraday mirror FM, which changes the polarization of the pulses by 90°. As the pulses travel back through modulator MA, Alice lets the first pulse P1 pass therethrough unmodulated but modulates the phase (i.e., imparts a phase shift Φ_A to) second pulse P2. It should be noted here that Alice could also choose to modulate pulse P1 so that this pulse is twice-modulated. Since pulses P1 and P2 are later interfered, it is not the phase imparted to each pulse that matters, but rather the relative phase between the two pulses. The modulation of pulse P1 at Bob and pulse P2 at Alice is described for the sake of example.

The timing of the modulation is provided by the synchronization signal SS shared between controllers 20 and 50, as described in greater detail below. The modulation at is carried at Alice out by controller 20 providing a well-timed signal S1 to RNG unit 16, which provides a signal S2 representative of a random number to voltage controller 14. In response, voltage controller 14 sends a voltage signal V_A (e.g., V[+3π/4], [V-3π/4], V[+π/4], and V[-π /4]) to modulator MA to set the phase modulation to a corresponding value +3π/4, -3π/4, π/4 or -π /4.

The two pulses P1 and P2 then travel back to Bob, where pulse P2 passes unaltered through modulator MB, but imparts a phase shift Φ_B to pulse P1. The timing of the modulation of pulse P1 at Bob is provided by the synchronization signal SS shared between controllers 20 and 50, as described in greater detail below. The modulation is carried out by controller 50 providing a well-timed signal S3 to RNG unit 46, which provide a signal S4 representative of a random number to voltage controller 44. In response, voltage controller 44 sends a voltage signal V_B (e.g., V[+π/4] or V[-π/4]) to modulator MB to set the phase modulation to a corresponding value +π/4 or -π /4.

Further, when pulses P1 and P2 enter M/D optical system 104, pulse P2 passes directly through but pulse P1 is delayed by an equal amount equal to that originally imparted to pulse P2. M/D optical system then interferes pulses P1 and P2.

The detectors 32a and 32b are arranged so that constructive interference ($\Phi_A - \Phi_B = 0$) is detected by detector 32a and destructive interference ($\Phi_A - \Phi_B = \pi$) is detected by detector 32b. When Bob imparts the same basis phase as Alice, a count in detector 32a indicates binary 0 and a count in detector 32b indicates binary 1. However, when Bob's basis phase is different from Alice's, there is no correlation and the count winds up in either detector 32a or 32b with equal probability (i.e., interfered the pulse has a 50:50 chance of being detected in either detector).

Modulator timing set-up

The description above relates to an idealized QKD system. However, in practice, such systems do not automatically operate in the ideal state. Further, a commercially realizable system must first be set up to operate and then must be able to compensate for changes in its operating state to ensure ongoing operation. The autocalibration methods set forth below presume that the modulator timing in QKD system 100 has been established.

Modulator autocalibration

As mentioned above, drifts can and do occur in the electronic layers of QKD systems during system operation. In a commercially viable QKD system, the drifts need to be automatically compensated so that the system can operate continuously. Accordingly, a method of performing modulator autocompensation is now described in connection with two-way QKD system 100.

With reference to FIG. 1 and to flow diagram 400 of FIG. 2, in 402 Bob provides a first select voltage —say V[π/4] – to phase modulator MB corresponding to one of the basis phases. This voltage depends on the type of

modulator, but may be, for example, 1 volt. Voltage V[π/4] sets modulator MB to a nominal phase setting of π/4.

Note that the voltages used to set the modulator to a select phase are each referred to below as a "basis voltage."

In 404, in an example embodiment, Bob sends pulses P1 and P2 through modulator MB over to Alice, who modulates one of the pulses and then sends the pulses back to Bob, where they are detected as an interfered pulse in detector 32a or detector 32b. During this process, Alice's voltage signal V_A for modulator MA is varied in the negative voltage range until the total phase shift imparted to the pulses is 0 (constructive interference). This is indicated by the pulses all being detected in detector 32a. This voltage is then set to be $V_A[-\pi/4]$.

It is worth noting that in 404, the pulses P1 and P2 returning to Bob from Alice are preferably weak (quantum pulses). However, these pulses could be strong pulses if used in combination with photodiode detectors arranged at Bob suitable for detecting strong pulses. For the sake of simplicity, however, quantum pulses are preferred, since the detectors in the system are single-photon detectors.

In 406, the voltage V_A provided to Alice's modulator MA is again varied, but in the positive voltage range, until the total phase shift imparted to the pulses is π (destructive interference). This is indicated by the pulses all being detected in detector 32b. This voltage is then set to $V_A[+3\pi/4]$.

At this point, Bob's voltage has been set at $V_B[\pi/4]$ and Alice's corresponding voltages $V_A[-\pi/4]$ and $V_A[+3\pi/4]$ have been established.

In 408, Bob's voltage is changed to the remaining voltage, which in this case is $V_B[-\pi/4]$. Acts 404 and 406 are then repeated to establish $V_A[\pi/4]$ by varying the positive voltage and to establish $V_A[-3\pi/4]$ by varying the negative voltage. Once this is accomplished, all of the (initial) voltages needed for modulating Bob's modulator MB and Alice's modulator MA are established.

In 410, pulses P0 are exchanged between Bob and Alice with fixed voltage settings that correspond to Bob making an "incorrect" basis measurement (i.e., the overall imparted phase to pulses P0 is not a multiple of π)

Bob's voltage is set to $V_B[\pi/4]$ and Alice is set at $V_A[\pi/4]$ so that Bob's modulator MB is set to $\pi/4$ and Alice's modulator is set to $+\pi/4$.

The distribution of counts in detectors 32a and 32b is then assessed, where detector 32a counts constructive interference and detector 32b counts destructive interference. Ideally, the count distribution should be equal since the probability of a count in each detector is 50:50 when Bob selects the incorrect phase basis.

In 412, if the number of counts in detector 32a is greater than that in detector 32b, then Bob's modulator voltage $V_B[\pi/4]$ is increased, and if it is less than that in detector 32b, then Bob's modulator voltage $V_B[\pi/4]$ is decreased. If the number of counts is found to be equal, then the method proceeds directly to 416.

In 414, acts 406 through 408 are repeated to re-adjust Alice's voltages $V_A[-\pi/4]$ and $V_A[3\pi/4]$ to correspond to Bob's new voltage as adjusted in 412.

In 416, acts 410 and 412 are repeated for Bob's remaining voltage, i.e., $V_B[-\pi/4]$. If Bob's remaining voltage needs to be adjusted to equalize the count number between the detectors, then in 418 acts 406 through 408 are repeated to adjust Alice's corresponding voltages $V_A[\pi/4]$ and $V_A[-3\pi/4]$.

Steps 410 and 416 are repeated until the ideal 50:50 detector count distribution is achieved,

Performing the above acts yields calibrated voltages for Bob's modulator MB and Alice's modulator MA. The QKD system is now ready for ideal operation. For security reasons, the above-described timing set-up and autocalibration procedures are preferably performed when Alice and Bob and optical fiber link FL are all in a secure location so there is no eavesdropper to alter the calibration. However, for the sake of necessity, the above-described procedures may need to be performed in the field even though this presents a security risk.

On-going modulator autocalibration

An example embodiment of the modulator autocalibration method of the present invention includes monitoring the counts in each detector that result from an incorrect basis measurement during the normal operation of the QKD system. As mentioned above, this count distribution should be 50:50 during system operation. After performing the QKD protocol, deviations from this count distribution can be used as a trigger to initiate the above-described autocalibration process so that it can be performed on an on-going basis.

In an example embodiment, the modulator timing set-up and autocalibration methods are accomplished by including software in controllers 20 and 40 that has instructions for carrying out the timing and autocalibration method discussed above and illustrated in the corresponding flow diagrams.

While the present invention has been described in connection with preferred embodiments, it will be understood that it is not so limited. On the contrary, it is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined in the appended claims.

MODULATOR AUTOCALIBRATION METHODS FOR QKD

ABSTRACT

Methods for autocompensating the modulators in a two-way QKD system are disclosed. The methods include setting Bob's modulator voltage to a positive value and then adjusting Alice's modulator voltage in both the positive and negative direction to obtain overall phase modulations that show up in one or the other of two detectors. Bob's modulator voltage is then set to a negative value and the process repeated. When all of the basis voltages are set, the QKD system is operated with purposely selected incorrect bases at Bob and Alice to assess whether the probability of photon detection is 50:50. If not, modulator voltages are adjusted and the technique repeated until a 50:50 detector count distribution is obtained for incorrect measurement bases.

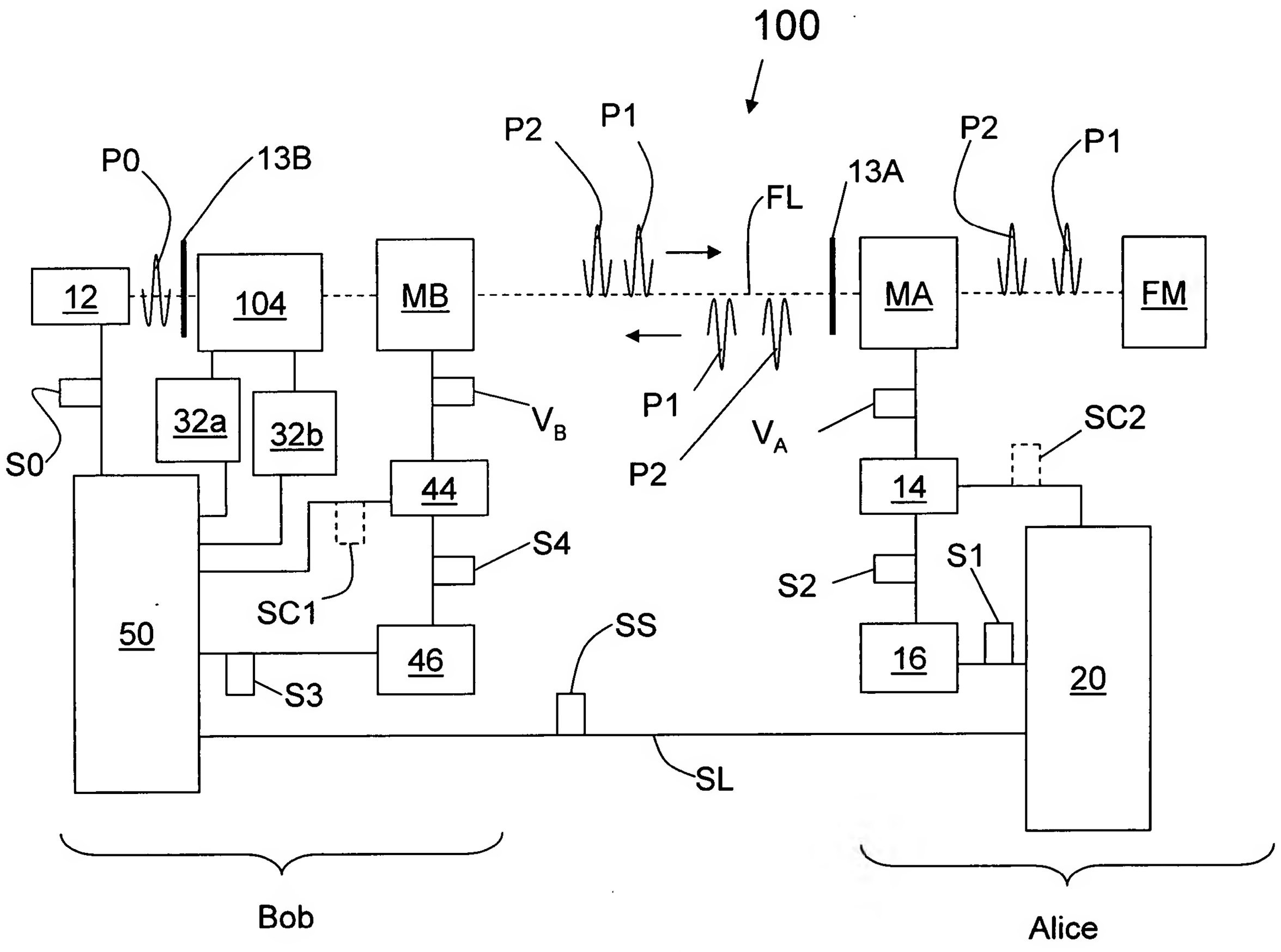
100
P0
13B
P2
P1
FL
13A
P2
P1
12
104
MB
MA
FM
P1
P2
V_B
V_A
S0
32a
32b
SC2
44
14
S4
S1
S2
SC1
SS
50
46
16
20
S3
SL
Bob
Alice

FIG. 1

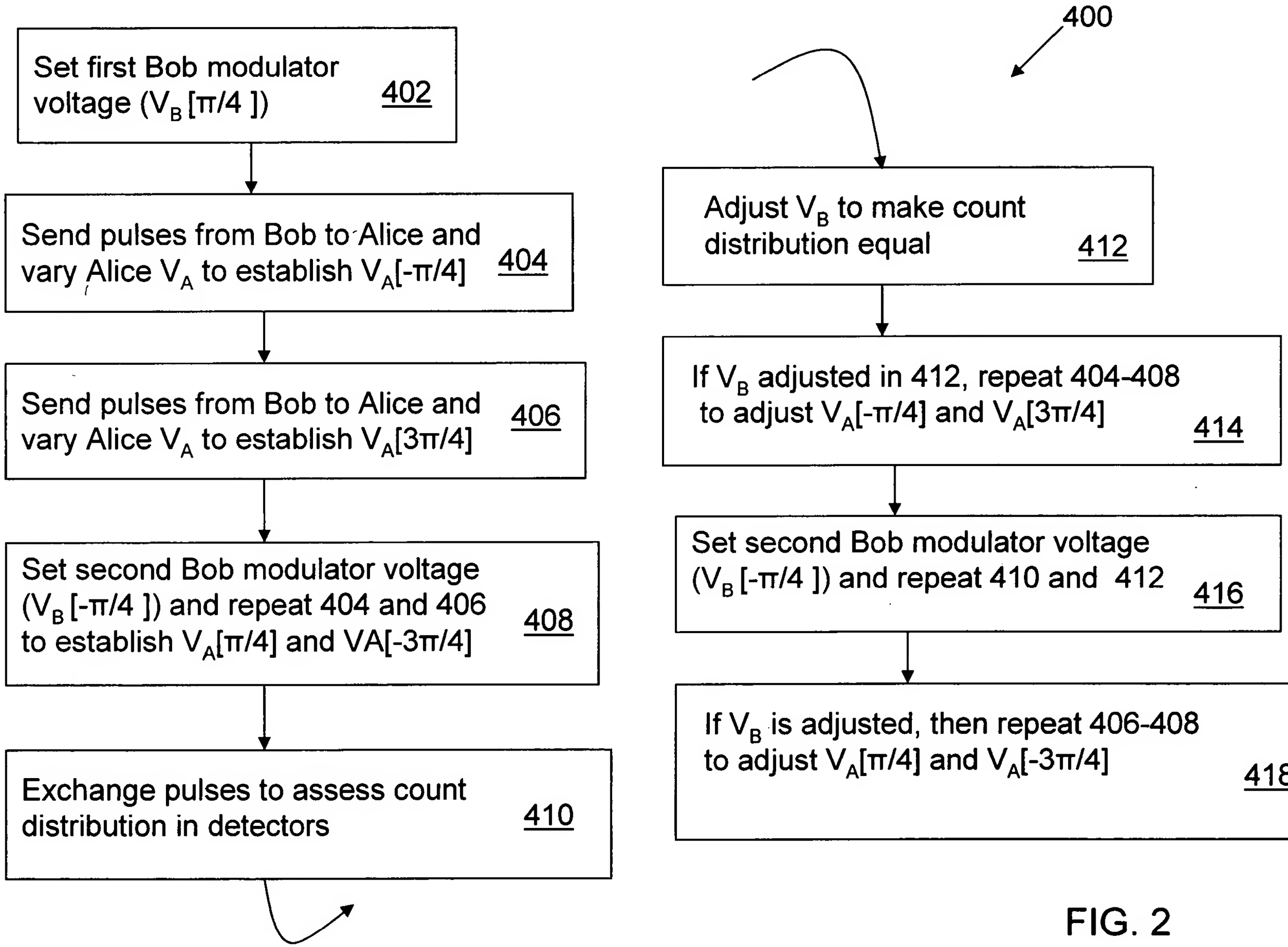
400
Set first Bob modulator voltage (V_B [π/4]) 402
Send pulses from Bob to Alice and vary Alice V_A to establish V_A[-π/4] 404
Send pulses from Bob to Alice and vary Alice V_A to establish V_A[3π/4] 406
Set second Bob modulator voltage (V_B [-π/4]) and repeat 404 and 406 to establish V_A[π/4] and VA[-3π/4] 408
Exchange pulses to assess count distribution in detectors 410
Adjust V_B to make count distribution equal 412
If V_B adjusted in 412, repeat 404-408 to adjust V_A[-π/4] and V_A[3π/4] 414
Set second Bob modulator voltage (V_B [-π/4]) and repeat 410 and 412 416
If V_B is adjusted, then repeat 406-408 to adjust V_A[π/4] and V_A[-3π/4] 418

FIG. 2